DOCKET NO. P04949 (NATI15-04949) PATENT
Customer No. 23990

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	HEZI FRIEDMAN ET AL.
Serial No.:	09/862,986
Filed:	May 22, 2001
For:	SECURE UNIVERSAL SERIAL BUS
Group No.:	2132
Examiner:	Kambiz Zand

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING BY FIRST CLASS MAIL

Sir:

The undersigned hereby certifies that the following documents:

1. Appeal Brief;
2. Fee Transmittal FY 2006 (in duplicate);
3. Check in the amount of $500.00 for the Appeal Brief Filing Fee; and
4. A postcard receipt;

relating to the above application, were deposited as "First Class Mail" with the United States Postal Service, addressed to Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on January 20, 2006.

Date: 1/20/06 Kathy Calder
Mailer

Date: Jan. 20, 2006 William A. Munck
Reg. No. 39,308

P.O. Drawer 800889
Dallas, Texas 75380
Phone: (972) 628-3600
Fax: (972) 628-3616
E-mail: wmunck@davismunck.com

PTO/SB/17 (12-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2006

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($) 500.00

Complete if Known	
Application Number	09/862,986
Filing Date	May 22, 2001
First Named Inventor	Hezi Friedman
Examiner Name	Kambiz Zand
Art Unit	2132
Attorney Docket No.	P04949 (NATI15-04949)

METHOD OF PAYMENT (check all that apply)

☑ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-0208 Deposit Account Name: Davis Munck, P.C.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☑ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent	50	25
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 20 or HP =	_____	x _____	= _____

HP = highest number of total claims paid for, if greater than 20

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 3 or HP =	_____	x _____	= _____

HP = highest number of independent claims paid for, if greater than 3

Multiple Dependent Claims Fee ($)	Fee Paid ($)
_____	_____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
_____ - 100 =	_____ / 50 =	_____ (round **up** to a whole number)	x _____	= _____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other: Appeal Brief	500.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 39,308	Telephone 972-628-3600
Name (Print/Type)	William A. Munck		Date Jan. 20, 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before application of:	Hezi Friedman *et al.*
Serial No.:	09/862,986
Filed:	May 22, 2001
For:	SECURE UNIVERSAL SERIAL BUS
Group No.:	2132
Examiner:	Kambiz Zand

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Applicants herewith respectfully submit that the Examiner's decision of August 23, 2005, finally rejecting Claims 2, 8-10, 13, 15, and 18-20 in the present application, should be reversed, in view of the following arguments and authorities. This Brief is submitted on behalf of Appellant for the application identified above. A check is enclosed for the fee for filing a Brief on Appeal. Please charge any additional necessary fees to Deposit Account No. 50-0208.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Real Party in Interest

The real party in interest, and assignee of this case, is National Semiconductor Corporation.

Related Appeals or Interferences

To the best knowledge and belief of the undersigned attorney, there are none.

Status of Claims

Claims 2, 8-10, 13, 15, and 18-20 are under final rejection, and are each appealed. Claims 6, 11, 12, 14, 16, and 17 were objected to in the final Office Action, and have been indicated by the Examiner as including allowable subject matter. Claims 3-5, 7, and 10, though rejected in the final Office Action, were objected to in the Advisory Action after amendment by the Applicant, and have been indicated by the Examiner as including allowable subject matter. Claim 1 was previously cancelled. Claims 2-20 are pending.

Status of Amendments after Final

The amendments to the claims made after final rejection have been entered, and are reflected in the Claims Appendix (Appendix A).

SUMMARY OF CLAIMED SUBJECT MATTER

The following summary refers to disclosed embodiments and their advantages, but does not delimit any of the claimed inventions.

In General

The present application is directed, in general, to apparatus and methods for providing a secure universal serial bus (USB). The secure USB comprises a secure channel for transferring data. A secure USB domain device is coupled to a host computer or is embedded within a host computer. The secure USB domain device comprises a USB memory device, a USB processor, a USB host

controller, and an internal USB bus coupled to each of the elements of the secure USB domain device. The elements of the secure USB domain device are not accessible by the host computer. The secure USB domain device blocks the transmission of confidential information, enables the transmission of non-confidential information, and enables the transmission of encrypted confidential information. *Abstract.*

Support for Independent Claims

Note that, per 37 CFR §41.37, only each of the independent claims are discussed in this section. In the arguments below, however, the dependent claims are also discussed and distinguished from the prior art. The discussion of the claims is for illustrative purposes, and is not intended to effect the scope of the claims.

Independent Claim 2 describes an apparatus for providing a secure serial bus (USB) comprising a secure channel for transferring data, wherein said apparatus comprises a secure USB domain device coupled to an external host computer, wherein said secure USB domain device comprises elements that are not accessible by said external host computer. *Page 13, lines 2-22; page 12, lines 2-6, and Figure 3b, below.*

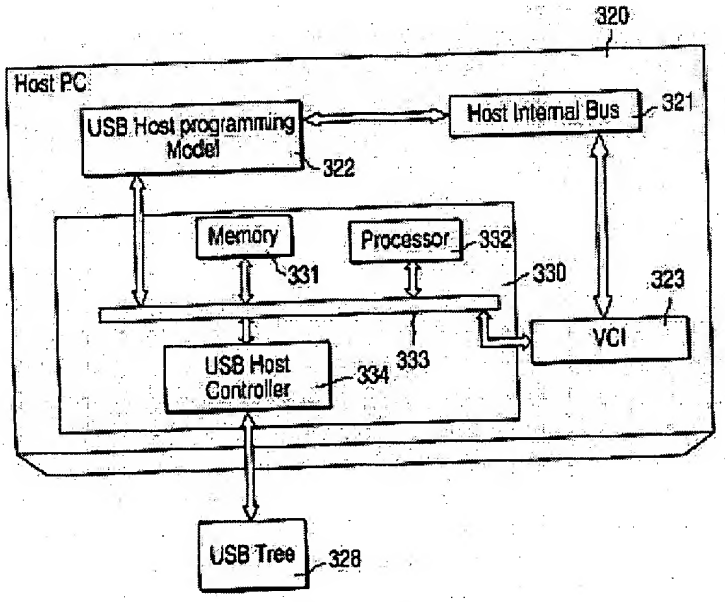


FIG. 3b

Independent claim 8 requires an apparatus for providing a secure universal serial bus (USB) capable of transferring information over a secure channel, said apparatus comprising: at least one host computer capable of supporting USB input/output devices, said at least one host computer comprising a USB bus, USB client software, and USB system software; and a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information. *Page 13, lines 2-22; page 12, lines 2-6, Page 21, line 17 - Page 22, line 17 and Figure 3b, above.*

Independent claim 15 requires a method for providing a secure universal serial bus (USB) capable of transferring information over a secure channel, said method comprising the steps of: providing at least one host computer capable of supporting USB input/output devices, said at least one host computer comprising a USB Bus, USB client software, and USB system software; and providing a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information. *Page 13, lines 2-22; page 12, lines 2-6, Page 21, line 17 - Page 22, line 17 and Figure 3b, above*

Grounds of Rejection to be Reviewed on Appeal

1. Is Claim 2 obvious over Rawlins (USP 6,216,183, "Rawlins")?

2. Are Claims 8-10, 13, and 15 obvious over Flannery (USP 5,799,196, "Flannery") in view of Rawlins?

3. Is Claim 20 obvious over Flannery in view of Rawlins in further view of Ben-Dor *et al.* (US2002/0141418A1, "Ben-Dor")?

4. Are Claims 18-19 obvious over Flannery in view of Rawlins in further view of Lemay *et al.* (US2002/0144115A1, "Lemay")?

ARGUMENT

Stated Grounds of Rejection

The rejections outstanding against the Claims are as follows:

In Section 9 of the August 23, 2005 Office Action, Claims 2 and 3 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,216,183, to Rawlins ("Rawlins"). In the Advisory Action, claim 3 was objected to and indicated as including allowable subject matter, and so claim 3 is not argued herein.

In Section 11 of the August 23, 2005 Office Action, Claims 8-10, 13, and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,799,196, to Flannery ("Flannery") in view of Rawlins.

In Section 12 of the August 23, 2005 Office Action, Claim 20 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Flannery in view of Rawlins and further in view of published patent application US2002/0141418A1 to Ben-Dor *et al.* ("Ben-Dor"). Applicant respectfully notes that the actual statement of rejection references claims 8-10, 13, and 15, but only claim 20 is addressed (and it is the only claim rejection that references Ben-Dor), so Applicant assumes that Examiner Zand intended to reference claim 20 here.

In Section 13 of the August 23, 2005 Office Action, Claims 18-19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Flannery in view of Rawlins and further in view of published patent application US2002/0144115A1 to Lemay *et al.* ("Lemay"). Applicant respectfully notes that the actual statement of rejection references only claim 18, but claim 19 is also discussed, so Applicant assumes that Examiner Zand intended to reference claims 18-19 here.

Legal Standards

The legal standards for an obviousness[1] rejection are referenced in the footnote below.

Analysis of Examiner's Rejection

The cited references are each briefly discussed in relevant part, and then the rejection of each claim is addressed separately under each ground of rejection.

Flannery, the primary reference used in the final Office Action, is drawn to a method and apparatus of providing power management using a self-powered universal serial bus (USB) device. Flannery discloses an alternative low power source can be combined with existing power management software that controls a computer's main power supply unit to provide stand-by power to logic in the computer that remains active to monitor the system environment for predetermined

---

[1]The Supreme Court has explained how to apply §103:

> Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or non-obviousness of the subject matter is determined.
>
> *Graham v. John Deere Co.*, 383 U.S. 1, 148 U.S.P.Q. 459, 467 (1966).

Obviousness cannot be inferred from a combination of references without a showing that one of ordinary skill would have been motivated to combine those references:

> When prior art references require selective combination ... to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight gained from the invention itself.... Something in the prior art as a whole must suggest the desirability, and thus the obviousness, of making the combination.
>
> *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 5 U.S.P.Q.2d 1434, 1438 (Fed.Cir. 1988), *quoting Interconnect Planning Corp. v. Feil*, 227 U.S.P.Q. 543 (Fed.Cir. 1985), *and Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick*, 221 U.S.P.Q. 481 (Fed.Cir. 1984).

wake-up events. A self-powered Universal Serial Bus device supplies the minimal power needed by the active logic without the inefficiencies of a dual-stage power supply unit or the expense of incorporating both low-power and a full-power units. . While Flannery shares some structural similarities with the instant application, it does not include several claimed elements and functions, as described in detail below, and as conceded by Examiner Zand.

Rawlins is drawn to an apparatus and method for securing information entered upon an input device coupled to a universal serial bus. Rawlins appears to have nothing to do with the power management techniques discussed in Flannery. Rawlins does address some security issues, but not in the manner contemplated by the claims, as described in detail below.

Ben-Dor is drawn to a system for tunneling between a bus, which can be a USB bus, and a network. Its only relevance appears to be that it mentions a "virtual USB host controller."

Lemay is drawn to methods and apparatus for downloading peripheral control code to a peripheral of a gaming device, for use in controlling one or more functions of the peripheral or for operation of the peripheral. The peripheral controller can be a USB controller. The data which is transferred in order to enable the peripheral and perform a verification or other functions may be encrypted

Ground of Rejection 1: Claims 2 was rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,216,183, to Rawlins ("Rawlins")

Claim 2

Claim 2 requires, "An apparatus for providing a secure serial bus (USB) comprising a secure channel for transferring data, wherein said apparatus comprises a secure USB domain device coupled to an external host computer, wherein said secure USB domain device comprises elements that are not accessible by said external host computer."

Rawlins's computer system (processor 12, system memory 18, northbridge 14) represents an external host computer. (*March 24, 2005 Office Action, Page 2, Line 24*). Southbridge 26 of

Rawlins's system comprises a PCI Interface Unit 28 and a USB Host Controller 30. Unlike the Host computer 100 in the present invention, host computer of the Rawlins system (processor 12) is able to access the USB Host Controller 30. Processor 12 operates in two different modes. The first mode is a normal operation mode. The second mode is a system management mode (SMM).

When the USB Host Controller 30 of Rawlins sends a system management interrupt signal (SMI) to processor 12, then processor 12 can access information that is stored within USB Host Controller 30. The processor 12 then switches from the normal operating mode to the system management mode (SMM). In the system management mode (SMM) the processor 12 switches to a separate operating environment contained within a system management random access memory (SMRAM). The SMRAM contains SMI handler code. The SMI handler code (under the control of processor 12) transfers information from the USB Host Controller 30 to a specified location within system memory 18. Therefore, the external host computer of Rawlins (processor 12, system memory 18, northbridge 14) is capable of accessing the information in USB Host Controller 30 whenever the processor 12 is operating in the SMM mode.

Examiner Zand stated that in the Rawlins system "there is no accessibility between the host and the USB device unless authorized, and no accessibility is allowed during normal operation." (*August 23, 2005 Office Action, Page 2, Lines 16-18*). This statement is not supported by Rawlins. In the Rawlins system there is no accessibility between the host (processor 12) and the USB device (USB Host Controller 30) during system management mode (SMM) of operation unless authorized by the USB Host Controller 30. Whenever the system management mode (SMM) mode of operation is activated, the host (processor 12) is able to access elements within the USB Host Controller 30. The Rawlins reference does not state that "no accessibility is allowed during normal operation." The fact that accessibility is allowed during secure operations does not imply that there is no accessibility during normal operations. In normal operations there is no need to restrict accessibility of the host (processor 12) to USB Host Processor 30. In any event, USB Host Processor 30 of Rawlins does comprise elements that are accessible by the host (processor 12) during the system management mode (SMM) of operation.

Therefore, claim 2 should be allowed over Rawlins, and Examiner Zand's obviousness rejection should be reversed.

Ground of Rejection 2: Claims 8-10, 13, and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,799,196, to Flannery ("Flannery") in view of Rawlins.

These claims are allowable over this combination of references, as discussed below.

Claim 8

Claim 8 requires at least one host computer capable of supporting USB input/output devices, said at least one host computer comprising a USB bus, USB client software, and USB system software; and a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information.

Flannery does describe a USB bus and software with relation to power management system. Examiner Zand concedes that Flannery does not teach or suggest a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information, as required by claim 8.

Examiner Zand instead references Rawlins's col. 2, lines 62-67 and col. 3, lines 1-18 for this teaching. This passage reads in its entirety:

> Upon receiving information from the USB keyboard, determination is made on whether that information is secured depending on whether the address associated with that information (i.e., DMA address) is from a monitored target endpoint address. The target endpoint address is an address of a USB device coupled to the host controller via the USB, and wherein the target endpoint device being monitored is

> maintained in one or more registers within the host controller. If a match occurs, then a control unit within the host controller will issue a SMI signal to the processor. The processor will then switch to a separate operating environment contained within a system management RAM (or SMRAM). The SMRAM contains what is often noted as SMI handler code. At least one function of the SMI handler code is to transfer the secured, keyboard-entered information (i.e., information from a monitored target endpoint address of a USB device) to a specified location within system memory. That location is accessible only while SMI is asserted, or during system management mode (SMM). In this fashion, the password entered upon the keyboard is contained within a secured portion of system memory not accessible during normal operation of the computer system, and certainly not accessible to an unauthorized user who is not privy to the endpoint addresses stored within the target endpoint address registers. Not knowing those addresses, or how the registers are configured during boot-up, or during subsequent re-configuration via a USB "control packet", unauthorized access is not allowed--especially since all USB transfers, including control transfers, bulk transfers in general, isochronous transfers and interrupt transfers can be trapped to allow generation of an SMI which, in turn, protects any hardware resource against unwarranted intrusion.

Nothing in this passage, or any other part of Rawlins, appears to teach or suggest a secure USB domain device capable of blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, or forwarding outgoing data flows of non-confidential information, as required by claim 8.

Further, even if such a teaching were found in one or another reference, there is no proper motivation to combine these references, as discussed more fully below, and no showing that such a combination would even be operable.

As such, Examiner Zand's rejection should be reversed, and claim 8 should be allowed over the art of record.

Claim 9

Claim 9 requires that the secure USB domain device of claim 8 comprises a plurality of USB devices; a first set of data channels for exchanging data with each of said plurality of USB devices; and a second set of data channels for exchanging data with said at least one host computer.

As claim 9 depends from claim 8, the arguments above with regard to claim 8 apply here as well, and are incorporated herein by reference.

Examiner Zand concedes that Flannery does not teach the additional limitations of claim 9. Examiner Zand refers instead to Rawlins's Figure 1 and associated text. While Rawlins's Figure 1 does show USB devices connected to communicate with the host system, nothing in Rawlins teaches or suggests a secure USB domain device that includes all the features of both claim 8 and claim 9.

Further, even if such a teaching were found in one or another reference, there is no proper motivation to combine these references, as discussed more fully below, and no showing that such a combination would even be operable.

As such, Examiner Zand's rejection should be reversed, and claim 9 should be allowed over the art of record.

Claim 10

Claim 10 requires that the secure USB domain device of claim 8 is embedded within said at least one host computer.

As claim 10 depends from claim 8, the arguments above with regard to claim 8 apply here as well, and are incorporated herein by reference.

Nothing in Flannery or Rawlins teaches or suggests a secure USB domain device that includes all the features of both claim 8 and claim 10, as required.

Further, even if such a teaching were found in one or another reference, there is no proper motivation to combine these references, as discussed more fully below, and no showing that such a combination would even be operable.

As such, Examiner Zand's rejection should be reversed, and claim 10 should be allowed over the art of record.

Claim 13

Claim 13 requires that the secure USB domain device of claim 8 is external to and coupled to said at least one host computer.

As claim 13 depends from claim 8, the arguments above with regard to claim 8 apply here as well, and are incorporated herein by reference.

Nothing in Flannery or Rawlins teaches or suggests a secure USB domain device that includes all the features of both claim 8 and claim 13, as required.

Further, even if such a teaching were found in one or another reference, there is no proper motivation to combine these references, as discussed more fully below, and no showing that such a combination would even be operable.

As such, Examiner Zand's rejection should be reversed, and claim 13 should be allowed over the art of record.

Claim 15

Claim 15 requires A method for providing a secure universal serial bus (USB) capable of transferring information over a secure channel, said method comprising the steps of: providing at least one host computer capable of supporting USB input/output devices, said at least one host

computer comprising a USB Bus, USB client software, and USB system software; and providing a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information.

Flannery does describe a USB bus and software with relation to power management system. Examiner Zand concedes that Flannery does not teach or suggest providing a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information, as required by claim 15.

Examiner Zand instead references Rawlins's col. 2, lines 62-67 and col. 3, lines 1-18 for this teaching. This passage reads in its entirety:

> Upon receiving information from the USB keyboard, determination is made on whether that information is secured depending on whether the address associated with that information (i.e., DMA address) is from a monitored target endpoint address. The target endpoint address is an address of a USB device coupled to the host controller via the USB, and wherein the target endpoint device being monitored is maintained in one or more registers within the host controller. If a match occurs, then a control unit within the host controller will issue a SMI signal to the processor. The processor will then switch to a separate operating environment contained within a system management RAM (or SMRAM). The SMRAM contains what is often noted as SMI handler code. At least one function of the SMI handler code is to transfer the secured, keyboard-entered information (i.e., information from a monitored target endpoint address of a USB device) to a specified location within system memory. That location is accessible only while SMI is asserted, or during system

> management mode (SMM). In this fashion, the password entered upon the keyboard is contained within a secured portion of system memory not accessible during normal operation of the computer system, and certainly not accessible to an unauthorized user who is not privy to the endpoint addresses stored within the target endpoint address registers. Not knowing those addresses, or how the registers are configured during boot-up, or during subsequent re-configuration via a USB "control packet", unauthorized access is not allowed--especially since all USB transfers, including control transfers, bulk transfers in general, isochronous transfers and interrupt transfers can be trapped to allow generation of an SMI which, in turn, protects any hardware resource against unwarranted intrusion.

Nothing in this passage, or any other part of Rawlins, appears to teach or suggest a secure USB domain device capable of blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, or forwarding outgoing data flows of non-confidential information, as required by claim 15.

Further, even if such a teaching were found in one or another reference, there is no proper motivation to combine these references, as discussed more fully below, and no showing that such a combination would even be operable.

As such, Examiner Zand's rejection should be reversed, and claim 15 should be allowed over the art of record.

Therefore, Claims 8-10, 13, and 15 should be allowed over the combination of Flannery and Rawlins, and Examiner Zand's obviousness rejections should be reversed.

Ground of Rejection 3: Claim 20 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Flannery in view of Rawlins and further in view of published patent application US2002/0141418A1 to Ben-Dor et al. ("Ben-Dor").

As noted above, although the specific statement for this ground of rejection referred to claims 8-10, 13, and 15, and not to claim 20, because only claim 20 was then discussed, Applicant assumes that Examiner Zand intended to reject only claim 20 over this combination of art. However, it should be noted that Ben-Dor fails to supply the teachings of claims 8-10, 13, and 15 not found in Flannery or Rawlins, as discussed above.

Claim 20

Claim 20 requires that the method of claim 15 further comprises the steps of coupling a virtual conduit interface to said secure USB domain device; coupling said virtual conduit interface to at least one non-USB device; and using said virtual conduit interface to provide a secure USB channel for transferring information to said at least one non-USB device.

As claim 20 depends from claim 15, the arguments above with regard to claim 15 apply here as well, and are incorporated herein by reference.

Examiner Zand concedes that these limitations are not taught or suggested by Flannery or Rawlins, alone or in combination.

Ben-Dor describes a virtual USB Host Controller that communicates between a USB bus driver and a network stack. However, the USB bus driver is not described as being a secure USB domain device as in claim 15, and there is no motivation, teaching, or suggestion to modify Ben-Dor's system to meet the claim limitations.

Further, even if such a teaching were found in one or another reference, there is no proper motivation to combine these references, as discussed more fully below, and no showing that such a combination would even be operable.

As such, Examiner Zand's rejection should be reversed, and claim 20 should be allowed over the art of record, and Examiner Zand's obviousness rejection should be reversed.

Therefore, all claims should be allowed over the combination of Watanabe and Glider, and Examiner Mason's obviousness rejections should be reversed.

Ground of Rejection 4: Claims 18-19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Flannery in view of Rawlins and further in view of published patent application US2002/0144115A1 to Lemay et al. ("Lemay").

These claims are allowable over this combination of references, as discussed below.

Claim 18

Claim 18 requires, among other limitations, that secure information is transferred between said at least one host computer and said secure USB domain device in a enciphered form, thereby establishing at least one secure data channel between said at least one host computer and said secure USB domain device.

As claim 18 depends from claim 15, the arguments above with regard to claim 15 apply here as well, and are incorporated herein by reference.

Examiner Zand concedes that these limitations are not taught or suggested by Flannery or Rawlins, alone or in combination.

Lemay describes a method and apparatus for downloading code, but has nothing at all to do with a secure USB domain device as in claim 15, and there is no motivation, teaching, or suggestion to modify Lemay's system to meet the claim limitations.

Further, even if such a teaching were found in one or another reference, there is no proper motivation to combine these references, as discussed more fully below, and no showing that such a combination would even be operable.

As such, Examiner Zand's rejection should be reversed, and claim 18 should be allowed over the art of record, and Examiner Zand's obviousness rejection should be reversed.

Claim 19

Claim 19 requires, among other limitations, that data flows from a first device to a second device directly through said secure USB domain device without utilizing resources of said host computer.

As claim 19 depends from claim 15, the arguments above with regard to claim 15 apply here as well, and are incorporated herein by reference.

Examiner Zand concedes that these limitations are not taught or suggested by Flannery or Rawlins, alone or in combination.

Lemay describes a method and apparatus for downloading code, but has nothing at all to do with a secure USB domain device as in claim 15, and there is no motivation, teaching, or suggestion to modify Lemay's system to meet the claim limitations.

Further, even if such a teaching were found in one or another reference, there is no proper motivation to combine these references, as discussed more fully below, and no showing that such a combination would even be operable.

As such, Examiner Zand's rejection should be reversed, and claim 18 should be allowed over the art of record, and Examiner Zand's obviousness rejection should be reversed.

Therefore, all remaining claims should be allowed over the combination of Flannery, Rawlins, Ben-Dor, and Lemay, and Examiner Zand's obviousness rejections should be reversed.

Motivation to Combine or Modify[2]

As described above, each of the rejections includes one or another combination of the Flannery, Rawlins, Ben-Dor, and Lemay references. Examiner Zand provides a variety of statements alleging various "motivations" for combining these references. As described below, these alleged motivations are not supported by the art of record, and so these particular combinations of references are improper.

The rejection of Claim 3, and indeed all of the rejections, depends on a combination of Flannery's power management system and Rawlins's system for securing information received from a USB input device. Examiner Zand alleges multiple "motivations" combining these references.

First, in page 4 of the August 25, 2005 final Office Action, Examiner Zand states that "[i]t would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize [in Flannery] the USB memory device, processor and host controller inaccessible to the host computer [alleged to be taught by Rawlins] so as to prevent unauthorized access to data by a

---

[2]Where an obviousness rejection is based on a combination of references, the Examiner must show that one of ordinary skill would have been motivated to combine those references. *See In re Nilssen*, 7 USPQ2d 1500 (Fed.Cir. 1988); *Panduit Corp. v. Dennison Mfg. Co.*, 1 USPQ2d 1593, 1597 (Fed.Cir. 1987); *ACS Hospital Systems v. Montefiore Hospital*, 220 USPQ 929 (Fed.Cir. 1984).

"When prior art references require selective combination ... to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight gained from the invention itself.... Something in the prior art as a whole must suggest the desirability, and thus the obviousness, of making the combination." *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 5 USPQ2d 1434, 1438 (Fed.Cir. 1988), *quoting Interconnect Planning Corp. v. Feil*, 227 USPQ 543 (Fed.Cir. 1985), *and Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick*, 221 USPQ 481 (Fed.Cir. 1984).

"While *[a reference]* may be capable of being modified to run the way *[the applicant's]* apparatus is claimed, there must be a suggestion or motivation in the reference to do so. See In re Gordon, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) ("The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification."). *In re Mills,* 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed.Cir. 1990).

malicious computer user." This motivation is unsupported by Flannery and Rawlins.

Flannery is concerned with USB power management, and describes a USB host that is coupled to a remote USB device located external to the computer. When the computer enters suspend mode, the main power supply unit is turned off but continually-powered logic remains active by drawing power from a second power source. When an external event occurs that requires processing by the computer, the remote USB device signals the continually-powered logic which then switches on the main power supply unit to resume the powered down logic.

Flannery doesn't discuss data transfer at all, or express any suggestion that "unauthorized access" is a problem. While Flannery makes general note that a USB hub or device transfers data, Flannery does not address at all the content of the data or indicate any need for securing it. Flannery discusses power supplies to internal and external USB devices. To combine Flannery with Rawlins according to Examiner Zand's stated motivation, one must believe that one of ordinary skill in the art is motivated to secure the power supply from an unauthorized user. Further, according to Rawlins's teachings, this would be accomplished by disconnecting host system power supply from the external device, which would clearly defeat the operation of Flannery's system completely. As such, the combination of Flannery's and Rawlins's alleged teachings is both unmotivated and would produce an inoperable invention.

Examiner Zand states a different, but similar, motivation in his rejection of claims 8-10 and 15. On page 6 and 7, Examiner Zand states that "[i]t would have been obvious to one of ordinary skilled [*sic*] in the art at the time the invention was made to utilize Rawlins's USB secure device [alleged to be] capable of blocking of confidential data in Flannery [*sic*] system in order to prevent leakage of confidential information. This motivation is as flawed as that above.

Flannery is not concerned with the "leakage" of confidential information, and does not even discuss confidential information or any other data security issues. Flannery describes a method and apparatus of providing power management using a self-powered universal serial bus (USB) device. Examiner Zand's stated motivation appears to be that one of skill in the art, when designing a power management system for a USB device, would also suddenly be inspired to stick some sort of data

blocking device in the system. Further, as above, the Rawlins's alleged teachings relied upon by the Examiner would also indicate that "protected" power management system would disconnect the external USB device from the host system – rendering Flannery's system inoperable.

As such, all rejections relying on a combination of Flannery and Rawlins – and that includes all rejections – do not have a proper motivation to combine these references, and such a combination of references would make an inoperable invention.

In the rejection of Claim 20, Examiner Zand adds Ben-Dor's "tunneling" system to the Flannery/Rawlins combination, and states that "[i]t would have been obvious to one of ordinary skilled [*sic*] in the art at the time the invention was made to utilize Ben-Dor's above limitation [a "virtual conduit interface"] in Flannery in view of Rawlins in order to allow for the USB controller to interface with non-USB hardware."

Ben-Dor does not teach or suggest – or even mention a "virtual conduit interface", as alleged by Examiner Zand. Ben-Dor mentions virtual drivers, and in the passage cited by Examiner Zand, mentions a "virtual USB host controller."

Flannery is concerned with a method and apparatus of providing power management using a self-powered universal serial bus (USB) device. Applicant is unable to imagine what kind of "virtual conduit interface", as described by the Examiner, or "virtual USB host controller", as described by Ben-Dor, would provide power to a USB device. No person of skill in the art, in designing Flannery's power management system, would then look for any teaching regarding a "virtual conduit interface" or "virtual USB host controller, and no such "virtual conduit interface", or "virtual USB host controller" for power delivery or management is believed to be operable.

Of course, it is also difficult to imagine how Flannery's power management teachings could apply at all to a "virtual USB host controller" as in Ben-Dor.

This combination also has no proper motivation.

In the rejection of claim 18, Examiner Zand adds Lemay's method and apparatus for downloading peripheral control code to the peripheral of a gaming device to the Flannery/Rawlins combination, and states that "it would have been obvious to one of ordinary skilled [*sic*] in the art

at the time the invention was made to utilize Lemay et al's [*sic*] enciphering format features in Flannery in view of Rawlins to prevent the deciphering by an intruder. Again, Flannery is concerned with a method and apparatus of providing power management using a self-powered universal serial bus (USB) device. Examiner Zand appears to suggest that one of ordinary skill in the art would find it necessary to encrypt a power supply, and that for some reason an "intruder" will try to decrypt the power supply. This motivation is not found in the cited references.

Finally, in the rejection of claim 19, Examiner Rand discusses only Flannery and Rawlins, but this time states "[i]t would have been obvious to one of ordinary skilled [*sic*] in the art at the time the invention was made to utilize Rawlins utilization resources of said host computer in Flannery system in order to screen its outgoing flow and prevent access to the data from an unauthorized user." Since the language of the claim specifically indicates that the resources of the host computer are not utilized, the Examiner's statement of motivation teaches directly away from the claim language.

Accordingly, the references used by Examiner Zand in every one of the present rejections cannot be properly combined, as there is no motivation in the art to do so, and the combinations, if made, would appear to be inoperable.

Grouping of Claims

The claims on appeal do not stand or fall together, as may be seen from the arguments set forth below. Each claim has been argued separately under a separate subheading, and each claim should be considered separately. While the applicant recognizes that a formal statement regarding the grouping of claims is no longer required, each claim should be considered separately; or at the very least each claim which is argued separately in the preceding sections of this brief should be considered separately. Argument: The fact that the claims use different formulations (as detailed above) and/or have been argued separately, shows that, if their patentability is not considered separately, any adverse decision would show that the limitations of some claims had been unfairly ignored.

REQUESTED RELIEF

The Board is respectfully requested to reverse the outstanding rejections and return this application to the Examiner for allowance.

Respectfully submitted,
DAVIS MUNCK, P.C.

Date: Jan. 20, 2006

William A. Munck
Registration No. 39,308
Attorney for Applicant

P.O. Drawer 800889
Dallas, Texas 75380
Phone: (972) 628-3600
Fax: (972) 628-3616
E-mail: wmunck@davismunck.com

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Hezi Friedman *et al.*
Serial No.:	09/862,986
Filed:	May 22, 2001
For:	SECURE UNIVERSAL SERIAL BUS
Group No.:	2132
Examiner:	Kambiz Zand

APPENDIX A -
Claims Appendix

1. (Cancelled)

2. (Previously Presented) An apparatus for providing a secure serial bus (USB) comprising a secure channel for transferring data, wherein said apparatus comprises a secure USB domain device coupled to an external host computer, wherein said secure USB domain device comprises elements that are not accessible by said external host computer.

3. (Previously Presented) The apparatus as claimed in Claim 2 wherein said secure USB domain device comprises:

a USB memory device that is not accessible by said host computer;

a USB processor that is not accessible by said host computer;

a USB host controller that is not accessible by said host computer; and

an internal USB bus that couples said USB memory device, said USB processor, and said USB host controller.

4. (Previously Presented) The apparatus as claimed in Claim 3 further comprising a USB node coupled to said USB bus, said USB node capable of being coupled to a USB tree.

5. (Previously Presented) The apparatus as claimed in Claim 2 wherein said apparatus comprises a secure USB domain device embedded within a host computer.

6. (Previously Presented) The apparatus as claimed in Claim 5 wherein said secure USB domain device comprises:

a USB memory device that is not accessible by said host computer;

a USB processor that is not accessible by said host computer;

a USB host controller that is not accessible by said host computer; and

an internal USB bus that couples said USB memory device, said USB processor, and said USB host controller.

7. (Previously Presented) The apparatus as claimed in Claim 6 further comprising a virtual conduit interface coupled to said secure USB domain device and coupled to at least one non-USB device, said virtual conduit interface capable of providing a secure USB channel for transferring information to said at least one non-USB device.

8. (Previously Presented) An apparatus for providing a secure universal serial bus (USB) capable of transferring information over a secure channel, said apparatus comprising:

at least one host computer capable of supporting USB input/output devices, said at least one host computer comprising a USB bus, USB client software, and USB system software; and

a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information.

9. (Previously Presented) The apparatus as claimed in Claim 8 wherein said secure USB domain device comprises:

a plurality of USB devices;

a first set of data channels for exchanging data with each of said plurality of USB devices; and

a second set of data channels for exchanging data with said at least one host computer.

10. (Previously Presented) The apparatus as claimed in Claim 8 wherein said secure USB domain device is embedded within said at least one host computer.

11. (Previously Presented) The apparatus as claimed in Claim 10 wherein said secure USB domain device comprises:

a USB bus;

a memory coupled to said USB bus capable of storing each data packet that is at least one of sent from and received by said secure USB domain device, said memory containing a set of buffers, each of said buffers comprising data associated with at least one of: said at least one host computer and a device coupled to said at least one host computer;

circuitry coupled to said USB bus, said circuitry capable of forwarding commands and requests for information received in said secure USB domain device;

a processor coupled to said USB bus, said processor capable of at least one of: classifying data packets, controlling forwarding operations, and controlling encryption operations; and

a USB host controller coupled to said USB bus, said USB host controller capable of managing data flow between said at least one host computer and a plurality of USB devices.

12. (Previously Presented) The apparatus as claimed in Claim 11 wherein said apparatus further comprises a virtual conduit interface coupled to said secure USB domain device and coupled to at least one non-USB device, said virtual conduit interface capable of providing a secure USB channel for transferring information to said at least one non-USB device.

13. (Previously Presented) The apparatus as claimed in Claim 8 wherein said secure USB domain device is external to and coupled to said at least one host computer.

14. (Previously Presented) The apparatus as claimed in Claim 13 wherein said secure USB domain device comprises:

a USB bus;

a memory coupled to said USB bus capable of storing each data packet that is at least one of sent from and received by said secure USB domain device, said memory containing a set of buffers, each of said buffers comprising data associated with at least one of: said at least one host computer and a device coupled to said at least one host computer;

circuitry coupled to said USB bus, said circuitry capable of forwarding commands and requests for information received in said secure USB domain device;

a processor coupled to said USB bus, said processor capable of at least one of: classifying data packets, controlling forwarding operations, and controlling encryption operations; and

a USB host controller coupled to said USB bus, said USB host controller capable of managing data flow between said at least one host computer and a plurality of USB devices.

15. (Previously Presented) A method for providing a secure universal serial bus (USB) capable of transferring information over a secure channel, said method comprising the steps of:

providing at least one host computer capable of supporting USB input/output devices, said at least one host computer comprising a USB Bus, USB client software, and USB system software; and

providing a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information.

16. (Previously Presented) The method as claimed in Claim 15 wherein the step of providing a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information, comprises the steps of:

storing each data packet received by said secure USB domain device in a memory containing a set of buffers, each of said buffers comprising data associated with at least one of: said at least one host computer and a device coupled to said at least one host computer;

forwarding commands and requests for information received in said secure USB domain device;

classifying each data packet sent from said device coupled to said at least one host computer to said secure USB domain device to one of: a first data type that requires no intervention and a second data type that requires intervention according to a buffer association;

forwarding data packets of the first type that are originated at said device to said at least one host computer;

blocking data packets of the second type that contain confidential information;

forwarding data packets of the second type that contain encrypted confidential information; and

forcing any exchange of data between said at least one host computer and said device coupled to said at least one host computer to flow through said secure USB domain device.

17. (Previously Presented) The method as claimed in claim 16, wherein the step of blocking data packets of the second type that contain confidential information, and the step of forwarding data packets of the second type that contain encrypted confidential information, comprise the steps of:

interrogating a header of each data packet of the second type to reveal a type of information required;

transferring said information in an encrypted form if the information is required at another host computer for further actions; and

if said information is required for data verification:

blocking the data packet;

receiving verification information from said at least one host computer in an encrypted form;

decrypting said verification information;

comparing said decrypted verification information with information received from said device coupled to said at least one host computer; and

providing said at least one host computer with an indication verifying whether a match was detected.

18. (Previously Presented) The method as claimed in Claim 15, wherein secure information is transferred between said at least one host computer and said secure USB domain device in a enciphered form, thereby establishing at least one secure data channel between said at least one host computer and said secure USB domain device.

19. (Original) The method as claimed in Claim 15, wherein data flows from a first device to a second device directly through said secure USB domain device without utilizing resources of said host computer.

20. (Original) The method as claimed in Claim 15, further comprising the steps of:

coupling a virtual conduit interface to said secure USB domain device;

coupling said virtual conduit interface to at least one non-USB device; and

using said virtual conduit interface to provide a secure USB channel for transferring information to said at least one non-USB device.

DOCKET NO. P04949 (NATI15-04949) **PATENT**
Customer No. 23990

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Hezi Friedman *et al.*
Serial No.:	09/862,986
Filed:	May 22, 2001
For:	SECURE UNIVERSAL SERIAL BUS
Group No.:	2132
Examiner:	Kambiz Zand

APPENDIX B -
Copy of Formal Drawings

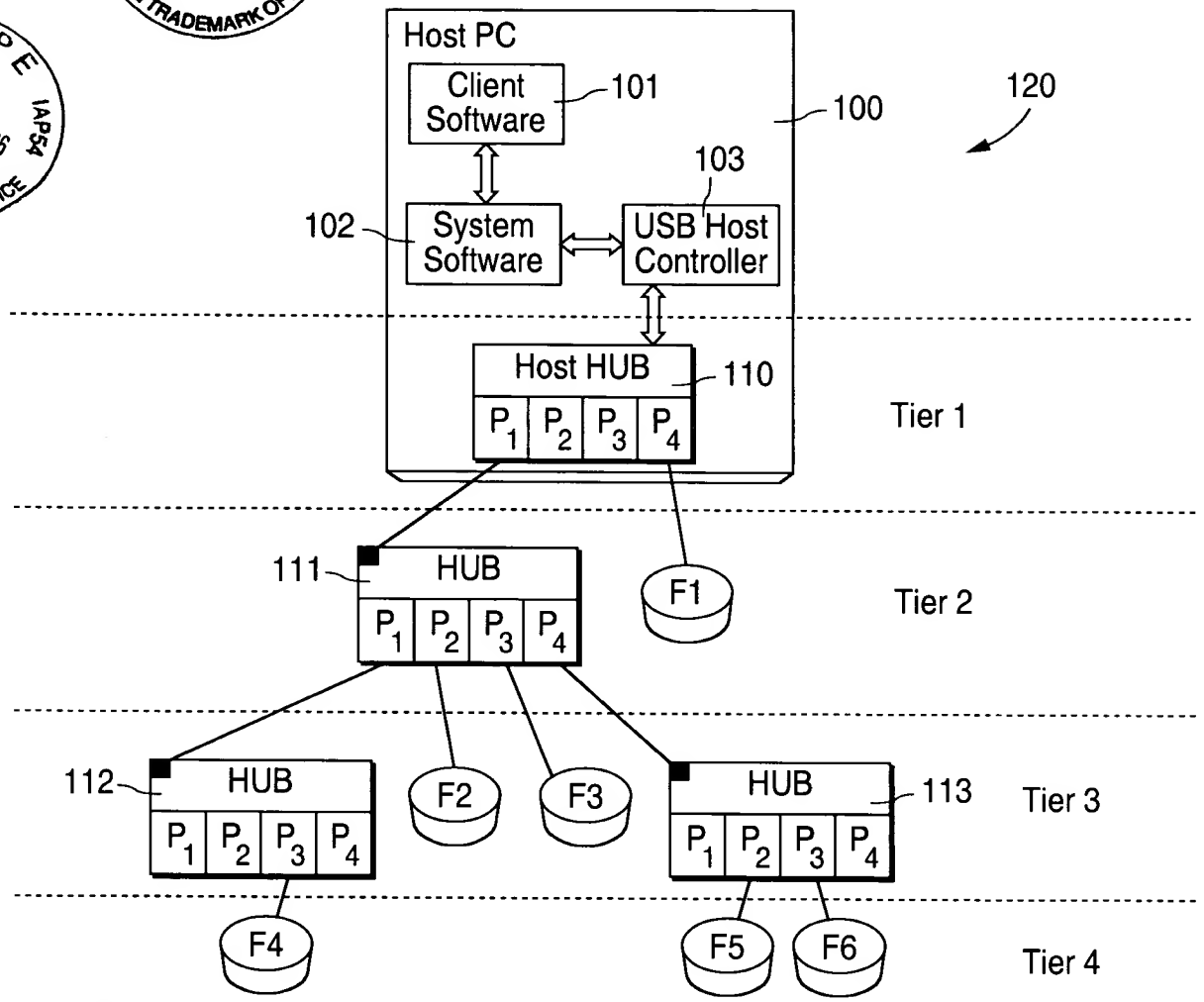


FIG. 1

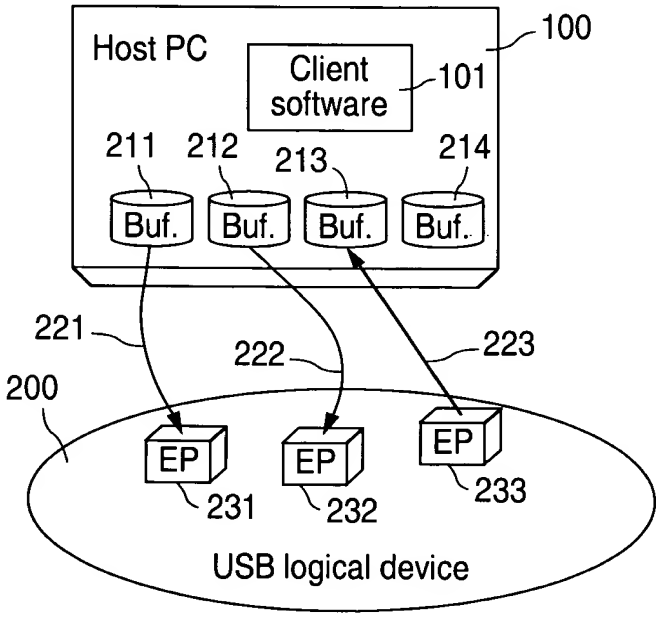


FIG. 2

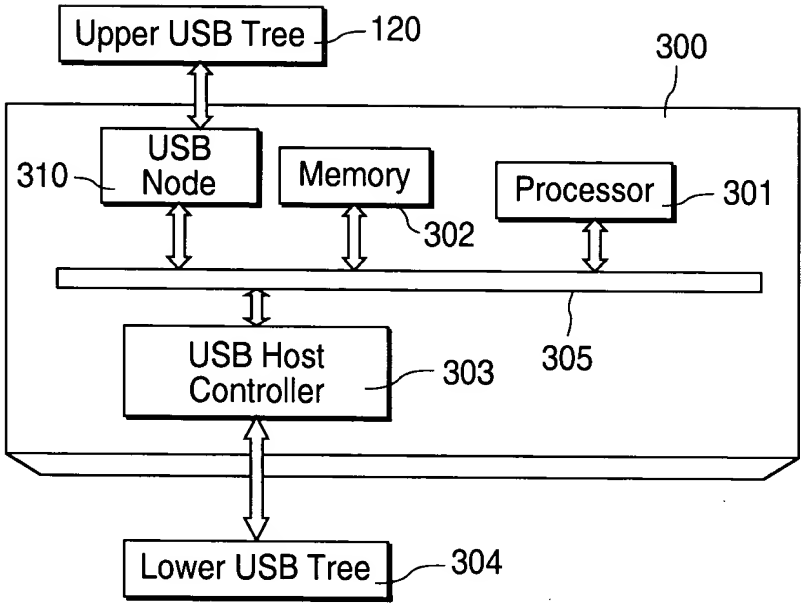

Upper USB Tree
120
300
USB Node
310
Memory
302
Processor
301
USB Host Controller
303
305
Lower USB Tree
304

FIG. 3a

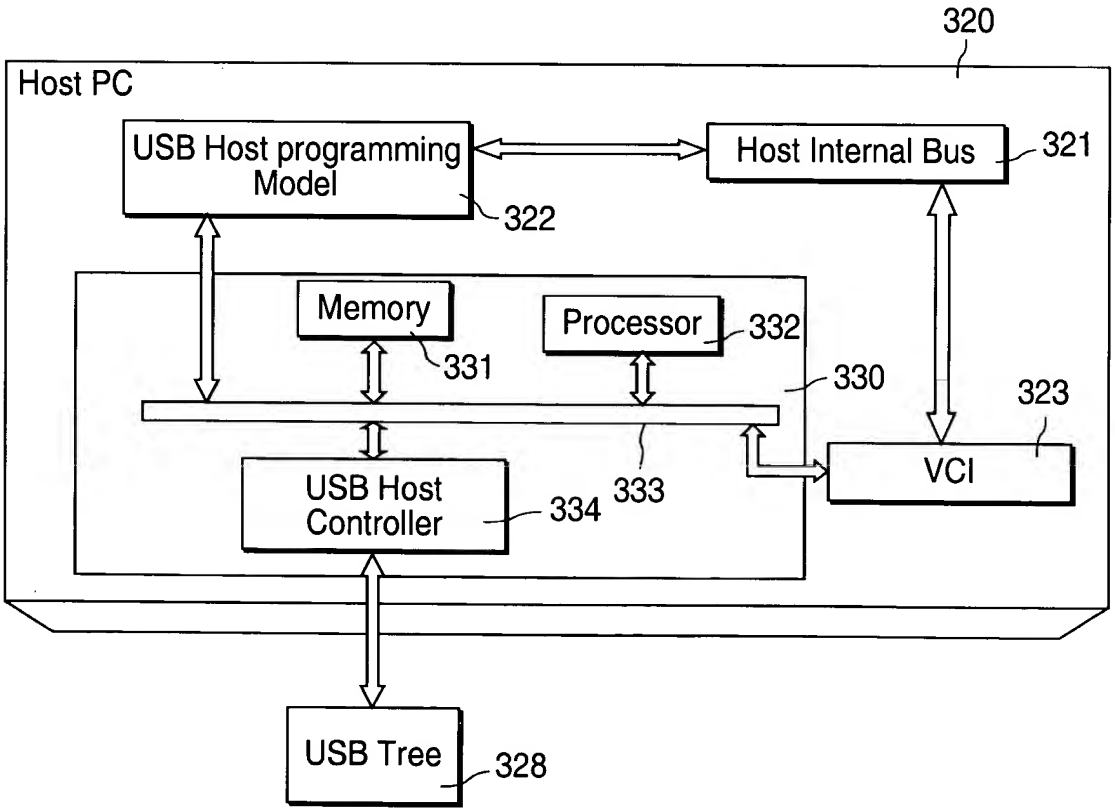

320
Host PC
USB Host programming Model
322
Host Internal Bus
321
Memory
331
Processor
332
330
323
VCI
USB Host Controller
334
333
USB Tree
328

FIG. 3b

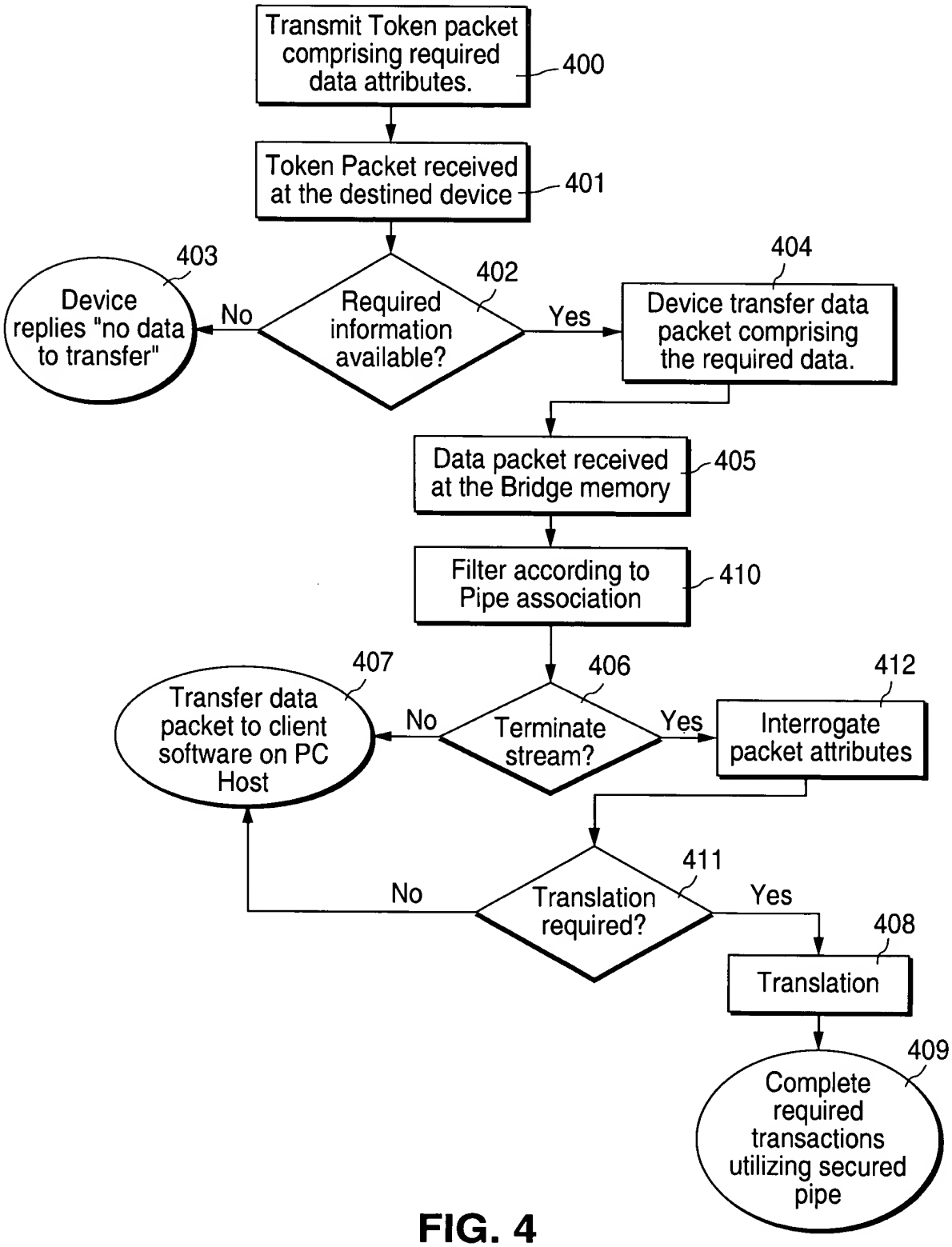
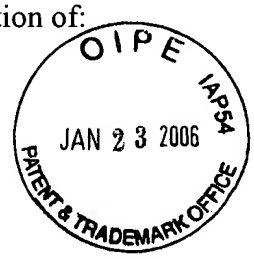

Transmit Token packet comprising required data attributes.
400
Token Packet received at the destined device
401
Required information available?
402
No
Yes
Device replies "no data to transfer"
403
Device transfer data packet comprising the required data.
404
Data packet received at the Bridge memory
405
Filter according to Pipe association
410
Terminate stream?
406
No
Yes
Transfer data packet to client software on PC Host
407
Interrogate packet attributes
412
Translation required?
411
No
Yes
Translation
408
Complete required transactions utilizing secured pipe
409

FIG. 4

DOCKET NO. P04949 (NATI15-04949) **PATENT**
Customer No. 23990

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



In re application of:	Hezi Friedman *et al.*
Serial No.:	09/862,986
Filed:	May 22, 2001
For:	SECURE UNIVERSAL SERIAL BUS
Group No.:	2132
Examiner:	Kambiz Zand

APPENDIX C -
Evidence Appendix

None.

DOCKET NO. P04949 (NATI15-04949) **PATENT**
Customer No. 23990

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Hezi Friedman *et al.*
Serial No.:	09/862,986
Filed:	May 22, 2001
For:	SECURE UNIVERSAL SERIAL BUS
Group No.:	2132
Examiner:	Kambiz Zand

APPENDIX D -
Related Proceedings Appendix

Not Applicable – To the best knowledge and belief of the undersigned attorney, there are none.